UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MICHIGAN Southern Division

D. G. Sweigert, Pro Se Plaintiff

-against-

MULTIMEDIA SYSTEM DESIGN, INC. d/b/a CROWDSOURCE THE TRUTH

A New York Corporation

ODYSEE HOLDINGS, INC. A Delaware Corporation

LBRY, INC. A Delaware Corporation

Defendant

CASE: 2:22-cv-10642-GAD

HON. G. DRAIN

Plaintiff Pro Se
D. G. SWEIGERT, C/O
MAILBOX, PMB 13339
514 Americas Way, Box
Elder, SD 57719
Spoliation-notice@mailbox.org

Defendant ODYSEE HOLDINGS, INC.

A New Hampshire Corporation

Defendant

MULTIMEDIA SYSTEM DESIGN, INC. d/b/a CROWDSOURCE THE

TRUTH

New York, New York 10001 truth@crowdsourcethetruth.org

Defendant LBRY, INC.

A New Hampshire Corporation

PUBLIC NOTICE OF DMCA TAKEDOWN

I hereby attest that the foregoing was transmitted on June 9, 2022 (6/9/22) under the penalties of perjury.

D. Jat

D. G. SWEIGERT, C/O MAILBOX,

PMB 13339, 514 Americas Way, Box Elder, SD 57719

PUBLIC NOTICE OF DMCA TAKEDOWN

NOW COMES D. G. SWEIGERT, *pro se* Plaintiff, to present artifacts under the penalties of perjury in preparation for seeking an emergency temporary restraining order. The Defendant is provided one last chance to comply with Section 512 of the Digital Millennium Copyright Act (D,M.C.A.).. The Court's attention is directed to the attached exhibits, certified authenticated as to their true nature by the undersigned.

D. 50

D. G. SWEIGERT, C/O AMERICA'S RV MAILBOX, PMB 13339 514 Americas Way, Box Elder, SD 57719 Spoliation-notice@mailbox.org

CERTIFICATE OF SERVICE

I, hereby certify, under penalties of perjury, that a true copy of the accompanying documents has been electronically forwarded with pdf copies to all parties listed below on June 9, 2022.

Jason Goodman truth@crowdsourcethetruth.org (as sole owner, sole employee, sole manager of CrowdSource The Truth the d/b/a for Multimedia System Design, Inc.) and "hello@odysee.com" <hello@odysee.com>, Julian <julian@odysee.com>, "josh@lbry.io" <josh@lbry.io>, Josh Finer <josh@odysee.com>, "legal@odysee.com" <legal@odysee.com>, "help@odysee.com" <help@odysee.com> "bjorn@odysee.com" <bjorn@odysee.com>, "abuse@odysee.com" dodysee.com "bjorn@odysee.com"

dodysee.com "bjorn@odysee.com"

dodysee.com "bjorn@odysee.com>, "abuse@odysee.com>, "abuse@odysee.com>, "abuse@odysee.com" dodysee.com "abuse@odysee.com">dodysee.com dodysee.com "abuse@odysee.com">dodysee.com dodysee.com <a

かっちって

June 9, 2022

D. G. SWEIGERT, C/O PMB 13339 514 Americas Way Box Elder, SD 57719 Spoliation-notice@mailbox.org

DMCA TAKE DOWN NOTICE

SUBMITTED JUNE 9, 2022

D. G. SWEIGERT, C/O
PMB 13339
514 Americas Way
Box Elder, SD 57719
Spoliation-notice@mailbox.org

TO:

DEFENDANT ODYSEE HOLDINGS, INC. of Manchester, New Hampshire Delaware Corporation 6098950, service via registered agent **HARVARD BUSINESS SERVICES, INC.** 16192 COASTAL HWY.

SUBJECT: D.M.C.A. takedown notice, notice of intent to sue.

Ladies and gentlemen:

LEWES, DELAWARE, 19958

- 1. This is your notification that a lawsuit to recover damages for copyright infringement has been brought against your firm.
- 2. The undersigned provides cyber security goods and services and owns the rights to professional papers that are distributed to research communities.
- 3. ODYSEE HOLDINGS, INC. owns and operates a video replay website known as "ODYSEE.COM" (the "Website").
- 4. ODYSEE HOLDINGS, INC. without permission or authorization from the undersigned actively copied, stored, and/or displayed the works of the undersigned on the Website and engaged in misconduct described in the attachment.

5. This notification also serves as your litigation hold and spoliation notice to preserve, archive and safely protect all evidence associated with the broadcast distribution of the above cited U.R.L. address. This includes all communications with the so-called "commentor" feature in the video "Jason Goodman" of New York City (presently a party in six (6) federal lawsuits). See:

https://news.bloomberglaw.com/ip-law/television-academy-wins-injunction-against-conspiracy-theorist

https://casetext.com/case/goodman-v-sharp-4

- 6. Pursuant to Section 512 of the Digital Millennium Copyright Act you are directed to remove the above cited video content described in the attachment

 (https://www.copyright.gov/512/) and inform the poster of your actions.
- 7. A copy of this letter shall be filed in litigation in which Mr. Goodman and your firm are parties to.

Respectfully,

D. G. Sweigert

D. Jat

Copy provided:

Jason Goodman, "C.E.O."

MULTIMEDIA SYSTEM DESIGN, INC.
d/b/a CROWDSOURCE THE TRUTH
A New York Corporation
252 7th Avenue, #6
New York, New York 10001
(323) 744-7594
truth@crowdsourcethetruth.org

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

Jason Goodman,

D/B/A CrowdSource The Truth

Plaintiff, CASE: 1: 21-cv-10878-AT-JLC

-against-

JUDGE TORRES

George Webb Sweigert,

Defendant.

Pro Se Intervenor
D. G. SWEIGERT, C/O
AMERICA'S RV
MAILBOX, PMB 13339
514 Americas Way, Box
Elder, SD 57719
Spoliation-notice@mailbox.org

Christopher Bouzy

Bot Sentinel

5101 Meadowview Ave,

North Bergen, NJ 07047

press@botsentinel.com

Plaintiff Pro Se JASON GOODMAN, CROWDSOURCE THE TRUTH

252 7th Avenue, #6 New York, New York 10001 (323) 744-7594

truth@crowdsourcethetruth.org

Defendant Pro Se

GEORGE WEBB SWEIGERT 1671 W. STEARNS ROAD, SUITE E TEMPERANCE, MI 48182 503-919-0748

Georg.webb@gmail.com

PROPOSED INTERVENOR'S SUPPLEMENT TO ECF NO. 27

I hereby attest that the foregoing was transmitted on May 31, 2022 (5/31/22) under the penalties of perjury.

D. 500

PROPOSED INTERVENOR D. G. SWEIGERT, C/O PMB 13339 514 Americas Way Box Elder, SD 57719

PROPOSED INTERVENOR'S SUPPLEMENT TO ECF NO. 27

I hereby attest that the attached public documents are true and accurate artifacts under the penalties of perjury.

D. G. SWEIGERT, C/O PMB 13339 514 Americas Way Box Elder, SD 57719

D. Jat

The foregoing document has been sent via e-mail message to:

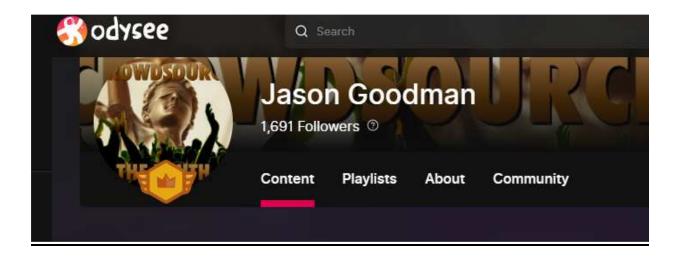
 $\underline{georg.webb@gmail.com}\;,\;\underline{press@botsentinel.com}\;and\;\underline{truth@crowdsourcethetruth.org}\;on$

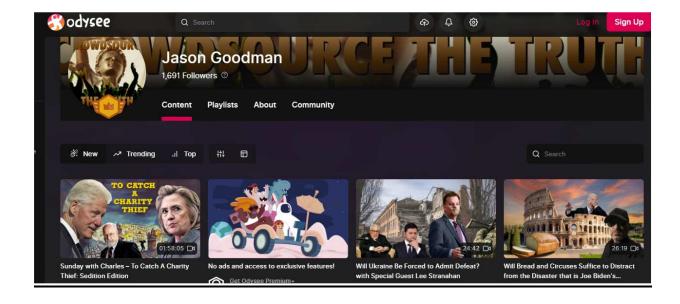
May 31, 2022, sworn under penalties of perjury

D. G. SWEIGERT

EXHIBIT ONE

https://odysee.com/@Crowdsourcethetruth:d





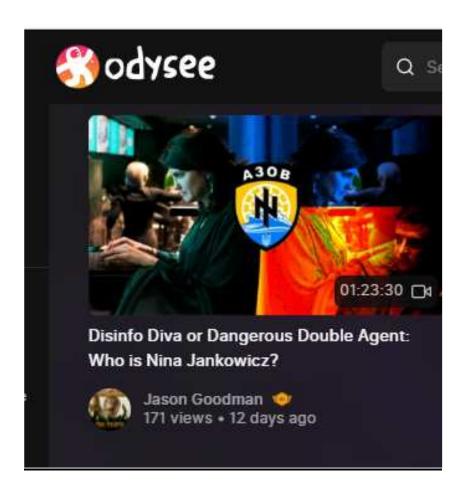


EXHIBIT TWO

https://odysee.com/@Crowdsourcethetruth:d/2022-05-16-20-00-03-Live:9



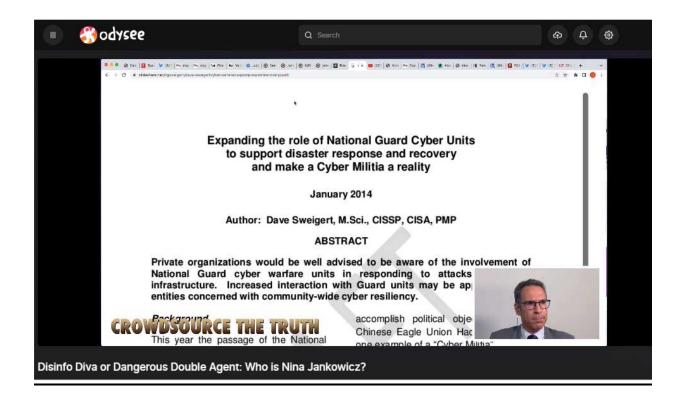


EXHIBIT THREE

https://www.slideshare.net/dgsweigert/davesweigertcyberwarfarecissppmprespondrecoveryppd8



Expanding the role of National Guard Cyber Units to support disaster response and recovery and make a Cyber Militia a reality

January 2014

Author: Dave Sweigert, M.Sci., CISSP, CISA, PMP

ABSTRACT

Private organizations would be well advised to be aware of the involvement of National Guard cyber warfare units in responding to attacks on critical infrastructure. Increased interaction with Guard units may be appropriate for entities concerned with community-wide cyber resiliency.

Background

This year the passage of the National Defense Authorization Act (NDAA) by the U.S. Congress (used to supply the Pentagon with another year's budget) came with cybersecurity strings attached – the requirement for a comprehensive domestic cyber warfare assessment of how the National Guard would support defensive cyber warfare operations and support missions of the U.S. Department of Homeland Security.

In sum, there is likely to be a new cybersecurity player in the Critical Infrastructure – Key Resources (CIKR) arena, the National Guard.

Is this the creation of a Cyber Militia?

Cyber Militias: these are non-state sponsored collections of volunteers that can act in a militant offensive and defensive manner in cyber space. These groups can be loosely organized and operate with technical know-how to

accomplish political objectives. The Chinese Eagle Union Hacker Group is one example of a "Cyber Militia".

Attacks launched by such groups that breach network cybersecurity are classified as "cyber warfare" by the Pentagon. Doomsday scenarios predict everything from massive failures of the power grid to the destruction of medical data as a consequence of an act of cyber war by such groups, creating "cyber anxiety".

Many observers have suggested that the language of the 2014 NDAA is a Dr. Strangelovian attempt to "close the cyber militia gap" and keep up with the creation of such militias in Russia, Iran, and North Korea.

Cyber Warfare: Both the National Guard Bureau (NGB) and the National Governor's Association (NGA) have openly endorsed the idea of Guard units engaged in civilian defensive cyber warfare operations.

Domestic Cyber Missions

Until now, the number of Guard units involved in civilian cybersecurity events could be counted with one hand. Examples:

Prior to the 2010 Winter Olympics the network supporting Washington State's Division of Motor Vehicles (DMV) was assessed by a Guard cyber warfare unit. supporting Networks the 2012 Presidential Inauguration were protected by such units and State networks supporting Emergency Management | (E.M.) activities have also been accessed by these groups.

Such activities fall within the **National**<u>Prevention</u> Framework "cybersecurity" category as a **PROTECTION** capability.

With the desire of Congress to "close the gap" the scope of such support by Guard units in domestic cyber missions could be expanding. Cascading consequences created by a cyber event are addressed within the National Response Framework as a RESPONSE and RECOVERY activity.

State Governors could certainly activate such units during man-made cyber disasters and to support response and recovery operations in natural disasters, as well as provide support to the U.S. Department of Homeland Security missions. However, only a handful of such states have these elite cyber warfare units.

Integration with the Whole Community Concept

The Whole Community Approach to Preparedness promoted by Presidential Policy Directive 8 (**PPD-8**: National Preparedness) is a comprehensive and integrated approach to community preparedness for disasters – to include man made cyber events and their cascading consequences.

The increased interaction of public safety agencies and private entities with these National Guard cyber units in support of **PPD-8** should be addressed by the Pentagon. Alignment of Guard cyber capabilities to jointly respond with other Whole Community partners in a realistic approach to a CIKR cyber event (and the associated potential downstream effects on public utilities, medical facilities, transportation arteries, etc.) should be planned for.

Joint planning would help define how these Guard units could more effectively interface with other response agencies during cyber events and disasters. This would give Congress the Cyber Militia capability they are searching.

About the author: Dave Sweigert holds certifications as a Certified Information Systems Security Professional, Certified Information Systems Auditor, and Project Management Professional. He earned Master's degrees in Information Security and **Project** Management. An Air Force veteran, he practitioner of cybersecurity, management incident and CIKR protection. He has consulted to Kaiser Permanente, J2 Global, NASA and the U.S. Army.